A Framework for Improving Security in Cloud Computing

Jayachander Surbiryala, Chunlei Li, Chunming Rong
Department of Electrical Engineering and Computer Science
University of Stavanger, Norway
e-mail: {jayachander.surbiryala, chunlei.li, chunming.rong}@uis.no

Abstract—**Cloud computing has been evolving over a couple of years with the increased use of cloud-based services like Amazon Web Services (AWS), Dropbox, Office 365, and so on. It revolves around the several technologies, for developing and supporting these services. With the evolution of new technologies, it leads to widespread use of cloud-based applications in real time. Processing powers are increased tremendously, more efficient, and centralized in the cloud environments. With the launch of services in a cloud environment has decreased the price of various services at the cost of security in these services. It is inevitable for most of the individuals and small organizations to use these services at reduced or less secured cloud services. There are many open challenges in the cloud environment, which needs to be addressed. In this paper, we propose a framework to solve various ethical and security aspects related to cloud computing.**

Keywords-cloud computing; framework; ethics; security

I. INTRODUCTION

Cloud computing is one of the areas in information technology (IT), many things change in the blink of an eye. There are many aspects of cloud computing; people tend to use as per their convenience. A lot of research is happening around cloud computing [1-4]. Cloud computing can affect the society, individuals, and firms in a way no one can imagine. However, it would be appropriate to think in security direction, how it is going to affect everyone if security in the cloud computing has not been taken seriously. It is suitable for everyone using the cloud services to understand the real security issues associated with these services.

In today's world, humans are marching towards the Internet of Things (IoT) [5] with many devices connected to the internet, the cloud can be used as one of the metaphors. Whereas, the internet is still the collection of servers (can be treated as devices) which are well connected through fiber optic cables or through some other means to provide or share the data between the connected nodes or devices. In other words, it can be stated as personal devices connecting to remote devices to perform some operation without using or limited use of private infrastructure can be called as cloud computing. Which is entirely different when compared to the traditional use of resources to perform the same computations or operations.

This model helps the individuals and organizations who would not like to invest huge amounts for short-term purposes in the platform, infrastructure, and software. Cloud computing is a model which helps to reduce the cost of operations and pay for the services which are used for the required or used period of services.

With a shift in the business model from the traditional to the cloud-based environment, there will be scope for expansion or reduction of the resources as per the requirements at a faster rate and helps to handle the resources effectively and cost efficiently.

The paper is organized into seven sections: the first section is the Introduction. Section II presents details about cloud computing along with various delivery models, and deployment models, Section III talks about ethics with their analysis and considerations. In Section IV, a brief understanding of security in a cloud environment is presented. In Section V we discuss the ethical and security aspects related cloud. Section VI describes the proposed framework using homomorphic encryption for a cloud environment, along with applicability of proposed framework and finally Section VII draws the conclusion.

II. CLOUD COMPUTING

As per the National Institute of Standards and Technology (NIST) standards [6], there are five main characteristics which need to be available in any service to be treated as cloud service which is:

1) **On-demand self-service:** user can carry out operation whenever he wants to use the service without any interference from anyone else.
2) **Network access:** is accessible with any internet-connected device.
3) **Location independent resource pooling:** resources should be shared across the users irrespective of their location.
4) **Physical transparency:** user can change their resource capacity as per their requirement.
5) **Pay peruse:** customer need to be charged based on the resources used.

Cloud computing can be classified based on service delivery models or deployment models. **Figure 1. The NIST cloud definition framework** represents both models based on NIST cloud definition framework [6]. In the cloud, there are three kinds of service delivery models namely:

1) **Infrastructure as a Service (IaaS):** users rent out the infrastructure provided by service providers such as processing power, disk storage, network and other computing resources. The user can use this infrastructure for any of their purposes to develop their own platform and software applications.

978-1-5090-4499-3/17/$31.00 ©2017 IEEE

2) **Platform as a Service (PaaS):** users rent out the platform to perform various operations like developing and managing their own applications without any concern regarding infrastructure.
3) **Software as a Service (SaaS):** users rent out the software applications. They just use the service without worrying about infrastructure and platform.

Cloud services can be deployed in several ways such as:

1) **Private cloud model:** an organization with their infrastructure to set their own cloud services.
2) **Community cloud model:** infrastructure is shared among the several organizations with shared objectives.
3) **Public cloud model:** cloud service provider will provide the infrastructure for other organizations or normal people.
4) **Hybrid cloud model:** where two or more models will be combined to provide the services to users or organizations.

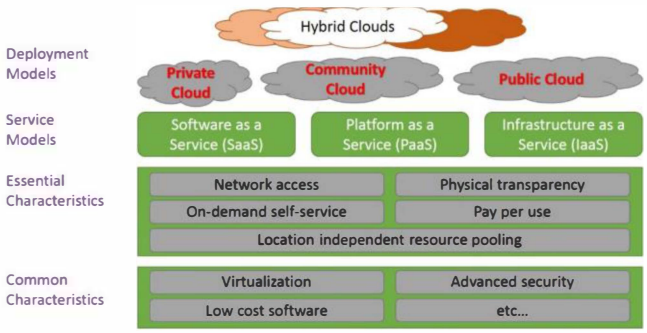

Figure 1. The NIST cloud definition framework [6]

Cloud Computing depends on various technologies, which exist in information technology even before the cloud service started to exist. An example of such technologies are virtualization and distributed processing. Any further improvements in these technologies will also support and boost the Cloud Computing. Some of the information technology organizations, even though they were using the underlying technologies, they might call their service as cloud services without following all the requirements mentioned above [7]. Sometimes cloud computing can be treated as some fancy word used to attract new customer base to sell their product. Such behaviour can be stopped by making international standards and making sure; every organization follows those standards. NIST has already released some standards; it is profitable if all the organizations follow these standards.

III. ETHICS

Ethics is one of the widely-studied topics in cloud computing after its introduction to the real world to store the information. Digital information has provided us with a lot of previous media information to understand the importance of it [8]. Cloud environment presents different ethical challenges that need to be understood properly, with unlimited access to the information, there is a probability that this information can be misused. Cloud computing is one of the things which leads to several debates on ethical aspects, as cloud environments have access to larger confidential information. Illegal or improper use of such data leads to ethical problems [9].

A. Ethical Analysis

Here we present the idea of ethics related to IT on various topics in connection to cloud computing. Readers who are more interested in in-depth details pertaining to the topic can refer the article [10]. IT systems lead to several issues related to ethical aspects.

Addressing the ethical aspects of cloud computing is somewhat complicated so, these issues can be dealt indirectly. There are three accepts that are appropriate for ethical analysis in cloud computing that plays a central role in addressing ethical issues of cloud computing are [11]:

1) **Control from technology to third parties for the cloud:** lead to loss of direct control in case of disasters like unauthorized access, infrastructure failure, or data loss.
2) **Multiple storage locations for redundancy:** can lead to privacy issues across the various border. For example, what happens if one of the storage location has been compromised with access to confidential data to an unauthorized person?
3) **The connection of services across different providers for a service in the cloud:** might lead to delays with an unexpected behaviour.

B. Dealing with Ethical Issues

Ethical issues in cloud computing include security and privacy which are obvious. It is evident that anyone will not be able to understand or identify all the ethical issues related to cloud computing. Like any normal person, cloud computing will also be facing real time scenarios that will be hard to determine. However, some basic understanding of ethical issues might help in real time scenarios in evaluating them to solve problems.

Being proactive about the ethical issues in cloud computing might solve some of the problems. In other words, we call it as the precautionary principle, which prevents the damage of unknown parameters without affecting the progress. For further knowledge on the precautionary principle, readers can refer to articles [12].

C. Ethical Frameworks

In this section, we will look into various theories related to ethics. These models make our analysis simple for making any decision. They are utilitarianism, and contractarianism are two approaches for analysis, which finds out whether the actions executed are correct or not [13].

Utilitarianism [13] works on the principle of utility, which states the ethically correct action is the outcome of the welfare of all concerned actions. In the ethical analysis, we often have several options. Utilitarianism will be useful

in such scenarios to evaluate those alternative options, by comparison, to produce the better result for each scenario.

On the contrary, contractarianism works with social contract [13], which serves as a counter-measure to utilitarianism. It works with the mutual agreement to get results for a person with the lesser concern of mutual service.

Another important concept is slippery slope reasoning [14]. Slippery slope presents with many problems in situations where decisions need to be taken. Sometimes it will be difficult to take decisions. It is better to avoid the contradictory frameworks like contractarianism and utilitarianism. Otherwise, we will end up with unimportant aspects for decision making as well.

As discussed in the previous subsection III-B, core precautionary principle can be used to compare the risks with respect to lesser worst outcome [15]. It can be used in scenarios where it is difficult to make any decisions based on utilitarianism and contractarianism. In some situations, we might not be able to predict the result so, it is appropriate to use ultraconservative precautionary principle. It says that any operation should be stopped if it is going to create any problem.

D. Ethical Considerations

For any of the ethical issues, the computer cannot be responsible; it should be an organization that provides the service will be responsible for those mistakes. That means the organization has not met the obligatory requirements to provide the services. Organizations providing services needs to understand the consequences of these mistakes.

If more than one approach is followed, it is better to choose their relation between them carefully. The ultraconservative precautionary principal is one of the most accepted principles in real time to solve the problems. In Section VI, we will present a new framework for the cloud environment, which can solve most of the issues.

IV. SECURITY

Security is a subjective topic according to ethical and social aspects. Security in the cloud is a process of securing data (or confidential information) from others getting access by interference or illegally without knowledge of the owner. Security in the cloud can be achieved in several ways depending on the type of controls used with the service. Many of the cloud service providers implement their own security controls to protect services and data associated with it. Sometimes organizations or paid users of the cloud services can choose security controls based on their requirements.

As discussed in the previous section some of the cloud services depend on many technologies, so security concerns associated with such technologies will still be applicable to the security issues in cloud computing. In other words, we can say that challenges faced by organizations using traditional services with other technologies are still applicable for cloud-based services. These security risks need to be managed properly and mitigated without any risk.

A. Security in Cloud

With the increased use and deployment of the cloud service, security issues in the cloud are also increasing. Organizations need to consider the following security issues in the cloud environment [16]:

- **Information in cloud computing environments:** can affect the organizations regarding security
- Aspects in the cloud. Based on confidential
- l information stored and processed in the cloud might lead various attacks.
- **Attackers and their capabilities:** attackers can be classified into internal and external attackers. The internal attacker has inside knowledge and access to many resources in the cloud. An external attacker might not have access to internal details but, they exploit vulnerabilities to attack cloud and gain access to confidential data.
- **Risk management in the cloud:** organizations need to understand the risk of moving to cloud environment in various aspects. Cloud service providers have access to their data, if it is not encrypted. For redundancy purposes, they store data on several servers. Deleting their data doesn't mean complete deletion of data on all servers and geographic location of these servers are unknown to the users or organizations using the cloud service.
- **New cloud security risks:** organizations need to be prepared for new types of attacks which might not exist in traditional systems such as side channel attacks, social networking attacks, mobile device attacks.
- **Existing cloud security issues:** need to be well understood, and proper defense mechanisms need to be implemented.

B. Standardization in Cloud Computing

For a proper understanding of security measures in a cloud environment, it is better to follow standardization in cloud environment across various cloud service provider. Some of the organizations working in cloud standardization are NIST cloud standards, Cloud Security Alliance (CSA), IEEE Standards Association (IEEE-SA), and International Telecommunication Union (ITU). IEEE-SA have formed two working groups *P2301 - cloud profiles* and *P2302 - intercloud* for improving standards to address migration, management, and interoperability across various cloud platforms. ITU has studied cloud computing and standardization under study group *13* [17].

V. ISSUES IN CLOUD COMPUTING

Cloud computing raises numerous ethical issue that arises when the control of the data is transferred from

provider to a third party. Therefore, there is a need to provide security and privacy for the users using cloud services, and to make it is possible for authorized persons to have control over the data.

Using cloud services, users exposed to several risks associated with their data, computation, and analysis. Cloud computing imposes challenges while transferring the data for any further action or analysis. Any such challenges need to be addressed and adequately discussed with users and cloud provider.

Security in IT is a combination of confidentiality, integrity, and availability known as CIA model.

1) **Confidentiality:** refers to access to the data to only authorized persons.
2) **Integrity:** related to the data modification is not possible.
3) **Availability:** ensures that data is accessible whenever it is required.

With the increased use of cloud services from various organizations and individuals, it is an ongoing process to meet the security requirements and get up to date security with the latest trend in technology. Authentication, authorization, and ownership (identification) are some of the main security concerns in cloud services.

Protection of data from unauthorized access is one more challenge. Data protection can be achieved with the help of proper data encryption protocols. As the data has to be exchanged over the internet, any attack possible on network protocols will be still applicable to confidential information in the cloud.

Another prominent issue in any IT system security is data availability. Cloud service provider needs to ensure the high availability of cloud services and data. Data needs to be protected from various factors including unforeseen circumstances without compromising security features like unauthorized access to the data in the cloud. Cloud provider needs to make sure of redundant backups in case of failures. It is better if the users and organizations using the cloud services have their own backup in regular intervals, in the case of any such emergencies. These backups can be used to verify the integrity of the data even if there is a failure in the cloud service provider.

Vulnerabilities and failures are common in any systems, which leads to security issues in the system. This is also applicable to the cloud services. Most of the issues can be easily identified and fixed based on their logging system management. Logs help in identifying, and isolating the problems where the issue has taken place.

One more problem with cloud based services is trust. Can an individual trust these cloud service providers with their personal and confidential data? How can customers be sure, service providers are not going to access the data and sell it to the third party?

VI. PROPOSED FRAMEWORK

To solve some of these issues in a cloud environment, we propose simple and yet powerful framework using homomorphic encryption of data to store and perform secure operations in the cloud. Gentry has proposed a fully homomorphic encryption [18] which allows us to carry computations on encrypted data (ciphertext), leads to encrypted results. When the results are decrypted will match the actions performed on plain data.

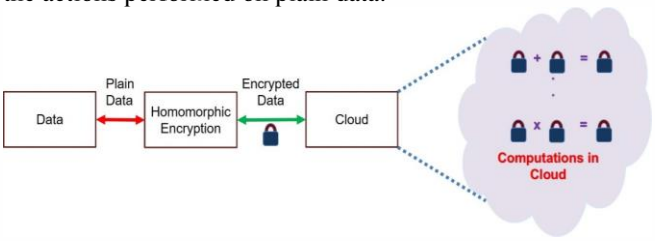

Figure 2. Overview of the proposed framework

Figure 2. Overview of the proposed framework shows the block diagram of the proposed framework to be implemented in a cloud environment. The proposed framework consists simple steps to achieve better security and solve many of the ethical and security issues in a cloud environment.

First, we need to encrypt the plain data using the homomorphic encryption technique. Once the data has been encrypted, we can store the data in the cloud. As the data is encrypted using homomorphic encryption, we can perform computations in the cloud. The computations carried on encrypted data will same as the computations carried on the plain data because of the usage of homomorphic encryption. To get the plain data from the cloud, we need to decrypt the data using the homomorphic method with same parameters.

A. Homomorphic Encryption

As shown in the Figure 2. Overview of the proposed framework, Homomorphic encryption allows us to perform the operations on encrypted data without decrypting in the cloud environment. A Fully Homomorphic encryption scheme should allow two basic operations on encrypted data without using the private key.

For example, if *m1*, *m2* are two messages and *Encrypt* and *Dcrypt* are encryption and decryption process defined for a Homomorphic encryption scheme then, following operations are valid.

$$\mathrm{C1} = \mathrm{Encrypt(m1)} \quad (1)$$

$$C2 = Encrypt(m2) \quad (2)$$

$$m1 + m2 = Dcrypt(C1 + C2) \quad (3)$$

$$m1 * m2 = Dcrypt(C1 * C2) \quad (4)$$

B. Applicability of Proposed Framework

If the cloud service providers adopt to the proposed framework using homomorphic encryption, it would solve some of the issues in the cloud but not limited to:

1) It provides security for the data stored in the cloud.
2) Confidentiality of the data stored in the cloud will be achieved.
3) Control and authorization of the data can be maintained as the parameters used for homomorphic encryption will only be known to the customer.
4) Unauthorized access to data might not lead to comprise of the information stored in the cloud.
5) Apart from all the issues addressed by the proposed framework, it allows customers to carryout computations on encrypted data in the cloud.

C. Reality

In cloud computing, most of the security measure need to be taken by cloud service provider. When data is stored, managed, processed, and analyzed in the cloud, security requirements are obligatory. Even security at physical locations needs to be considered. By adopting the proposed framework by big cloud service providers like Amazon EC2 [19], Google Cloud Platform [20], Microsoft Azure [21] will encourage customers to rely on them. Even though the idea of homomorphic encryption exists from a long time, it is still not developed entirely to adopt to cloud environments because of the complexity of operations involved to perform actions on encrypted data. Rapid increase in computation power possessed by cloud service providers, homomorphic encryption can be adopted in cloud environments.

VII. CONCLUSION

Cloud computing provides many advantages for individuals and small organizations; it can also create some serious security issues with personal and confidential data. Cloud service providers should take proper security measures to prevent all security related issues. We have proposed a simple yet powerful framework using homomorphic encryption for solving data security problems in cloud environments. Adoption of the proposed framework will solve many of the issues in cloud environment related to ethical and security aspects.

ACKNOWLEDGMENT

The authors are grateful to the anonymous reviewers for their constructive suggestions to improve the quality of the paper.

REFERENCES

[1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of internet services and applications, vol. 1, no. 1, pp. 7–18, 2010

[2] B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," INC, IMS and IDC , pp. 44–51, 2009

[3] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," Computers & Electrical Engineering, vol. 39, no. 1, pp. 47–54, 2013

[4] J. W. Rittinghouse and J. F. Ransome, Cloud computing: implementation, management, and security. CRC press, 2016

[5] R. H. Weber and R. Weber, Internet of Things. Springer,2010, vol. 12

[6] P. Mell and T. Grance, "Effectively and securely using the cloud computing paradigm," NIST, Information Technology Laboratory, pp. 304–311, 2009

[7] M. Spinola, "An essential guide to possibilities and risks of cloud computing," Retrieved March, vol. 24, p. 2011, 2009.

[8] V. Ratten, "Entrepreneurial and ethical adoption behaviour of cloud computing," The Journal of High Technology Management Research, vol. 23, no. 2, pp. 155–164, 2012.

[9] O. Freestone and V. Mitchell, "Generation y attitudes towards e-ethics and internet-related misbehaviours," Journal of Business Ethics, vol. 54, no. 2, pp. 121–128, 2004.

[10] S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," Government Information Quarterly, vol. 27, no. 3, pp. 245–253, 2010

[11] J. Timmermans, B. C. Stahl, V. Ikonen, and E. Bozdag, "The ethics of cloud computing: A conceptual review." 2010.

[12] W. Pieters and A. Cleeff, "The precautionary principle in a world of digital dependencies,"Computer, vol. 42, no. 6, pp. 50–56, 2009.

[13] A. P. Hamlin, "Rights, indirect utilitarianism, and contractarianism," Economics and philosophy, vol. 5, no. 02, pp. 167–188, 1989.

[14] S. Blackburn, Ethics: A very short introduction. Oxford University Press, 2003, vol. 80

[15] S. M. Gardiner, "A core precautionary principle," Journal of Political Philosophy, vol. 14, no. 1, pp. 33–60, 2006.

[16] CPNI. (2010) Cloud computing - information security briefing - 01/2010. [Online – Sept-2016]. Available: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf

[17] IEEE. Standards in cloud computing. [Online]. Available: http://cloudcomputing.ieee.org/standards

[18] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009

[19] Amazon Elastic Compute Cloud. [Online]. Available: https://aws.amazon.com/ec2

[20] Google Cloud Platform. [Online]. Available: https://cloud.google.com/

[21] Microsoft Azure. [Online]. Available: https://azure.microsoft.com.